홈 네트워크에서 안전한 콘텐츠 전송을 위한 DRM 시스템의 설계

이창보*, 이영구*, 이광형**,전문석*
*숭실대학교 대학원 컴퓨터 학과
**서일대학 인터넷정보과
e-mail: {onsmile79, ad3927}@ssu.ac.kr,
dreamace@seoil.ac.kr,
mjun@computing.ssu.ac.kr

Design of DRM System for Secure Content Delivery in HomeNetwork

Chang-Bo Lee*, Young-Gu Lee*, Kwang-Hyoung Lee**,
Moon-seog Jun*
*Dept of Computer Science, Soong-sil University
**Dept of Internet Information, Seoil College.

요 약

대부분의 DRM 시스템은 콘텐츠의 보호 위주로 발전하여 사용자가 콘텐츠 이용 시에 콘텐츠의 사용에 많은 제약사항이 따랐다. DRM이 적용된 콘텐츠를 DRM서버로부터 다운로드 받아 사용할 때에, 콘텐츠를 다운로드 받은 디바이스에서만 콘텐츠 이용이 가능하였고, 콘텐츠를 다른 디바이스로 옮기고 사용하기 위해서는 추가로 DRM 서버로부터 인증을 받아야 했다. 이것은 라이선스가 디바이스에 바인딩이 되었기 때문이다. 본 논문에서 제안하는 시스템은 다양한 홈 디바이스들을 하나의 도메인으로 묶어 같은 도메인안의 디바이스 간에는 자유롭게 콘텐츠 이동이 용이하게 하는 것이다. 지속적인 콘텐츠의 저작권 보호와 편리한 콘텐츠 사용 그리고 콘텐츠의 구매 비용을 절감 효과를 가져올 수 있다.

1. 서론

인터넷은 수많은 지식과 디지털 콘텐츠를 제공하는 허브로써 인터넷을 통해 쉽게 콘텐츠를 분배하고 사용하는 것이 가능해졌다. 그러나 이러한 콘텐츠의 편리한 분배 및 무분별한 복사는 디지털 콘텐츠를 만든 사람의 지적 재산권을 침해뿐 아니라 디지털 콘텐츠 시장의 전반을 위협할 수 있는 문제로 대두되었다. 이러한 문제를 해결하기 위해 방법으로 DRM(Digital Rights Management) 기술이 등장하였다. DRM 기술은 저작권 보호 기술을 이용하여 허가되지 않은 사용자로부터 디지털 콘텐츠를 안전하게 보호하고 유통전반을 감시, 추적하여 저작권의 권리 및 이익을 지속적으로 보호하고 관리하는 기술이다[2]. 그러나 이러한 DRM기술은 콘텐츠의 저작권을 보호할 수는 있지만 사용자가 콘텐츠를 사용하는데 있어 여러 가지 제한이 따를 수밖에 없다.

특히 DRM의 Superdistribution 기술은 사용자가 콘텐츠를 입수 하더라도 인증 받은 사용자만이 콘텐츠의 라이선스를 받아 콘텐츠를 사용 있는 기술이다. 이때 라이선스는 디바이스와 바인딩 되어 있으므로, 콘텐츠를 사용하기 위해서는 인증 받은 디바이스 외에 다른 디바이스에서 콘텐츠를 사용할 수 없게 된다. 결국 사용자가 콘텐츠 제공자로부터 구입한 콘텐츠는 최초에 다운로드받은 디바이스 외에 다른 디바이에서 콘텐츠를 사용하기 위해서는 DRM 서버로부터 다시 인증 받아야 하는 불편함이 생긴다.

본 논문에서는 사용자를 인증하기 보다는 디바이스를 인증하는 구조적인 문제점을 보완하고자, 사용자가 구입한 디바이스들 간에 도메인을 구성하고, 자동으로 라이선스를 재 패키징(re-package)하여 장치

* 본 연구는 서울시 산학연 협력사업으로 구축된 서울 미래형 콘텐츠 컨버전스 클러스터 지원으로 수행되었습니다.

들 간에 콘텐츠 공유를 자유롭게 하기 위한 새로운 DRM 프레임 워크를 제안한다.

2. 관련 연구

2.1 DRM 시스템의 구성

DRM 시스템은 (그림 1)과 같이 출판업자와 콘텐츠 공급업자, 사용자, 그리고 클리어링 하우스(Clearing house)등으로 구성되고 세부 기능은 다음과 같다[5].

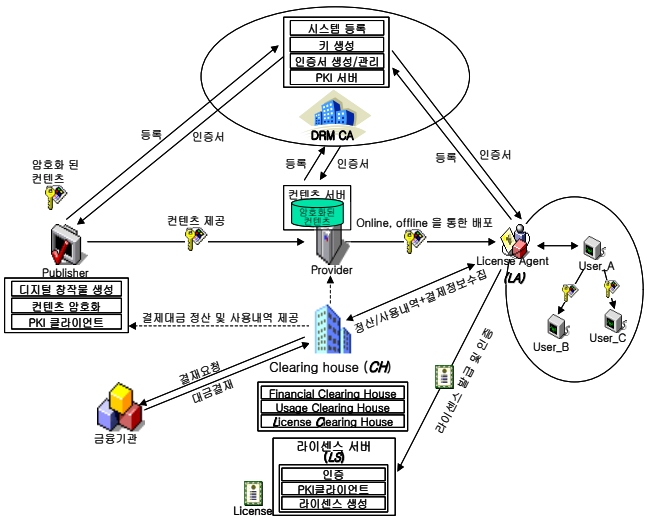

그림 1. DRM 시스템의 구성

전체 DRM 시스템의 참여자들은 DRM CA로부터 공개키를 등록하고 인증서를 발급 받는다. 콘텐츠 출판업자는 콘텐츠 제공자에게 보호조건, 저작권, 사용조건, 인증 정보, 사용 비용, 사용 추적 조건 등을 명시하고 분배 업자에게 전송한다. 콘텐츠 분배 업자는 출판업자가 제공한 보호조건에 맞도록 암호화하여 암호화된 콘텐츠를 생성한다. 암호화된 콘텐츠는 콘텐츠를 이용하고자 하는 사용자에게 온라인 혹은 오프라인을 통하여 배포된다. 또한 분배 업자는 콘텐츠에 대한 가격, 결제 처리 방법 등을 정한 후 해당 정보를 데이터베이스에 저장하고 클리어링 하우스에 전송하여 사용자에 대한 결제 정보를 처리할 수 있도록 한다. 사용자는 온라인이나 오프라인을 통해 다운로드 받은 콘텐츠는 암호화 되어 있기 때문에, 콘텐츠를 이용하기 위해서 라이선스 에이전트를 통해 클리어링 하우스로부터 라이선스를 발급받고 해당 라이선스를 클리어링 하우스를 통하여 인증한 후 결제 정보를 제공하면 라이선스 에이전트가 콘텐츠를 사용할 수 있도록 처리를 수행하게 된다.

2.2 라이선스 구조

라이선스는 라이선스 일련 번호 sn, 라이선스 발행시간 date, 사용규칙 Usage rule, 라이선스 하드웨어 바인딩 정보인 KID = H(DID||LSID), 기타 필요한 정보를 포함한 Other_data를 포함한다. 여기서 DID는 사용자의 하드웨어 장치 ID를, LSID는 라이선스 서버의 ID를 의미한다. 무결성, 부인방지를 위해 이러한 파라미터들을 해쉬 함수 H로 처리하고 라이선스 서버의 개인키로 암호화 하여 서명을 한다[5].

License = {sn, KID, date, Usage rule, other_data, SigLS(H(sn, KID,date, Usage rule, other_data))}

3. 제안한 시스템의 프레임워크

집에서 각종 디바이스를 소유하고 있는 사용자는 도메인을 설정한다[1]. 그리고 디바이스를 도메인에 등록 시켜야 한다. 같은 도메인 안에 존재하는 디바이스들은 콘텐츠 이동시 자동으로 같은 도메인에 포함된 디바이스인지 인증을 거쳐 라이선스를 재패키징(re-packaging) 하여 콘텐츠와 라이선스를 보내주어야 한다.

3.1 제안한 DRM 시스템의 요구사항

제안하는 DRM 시스템은 모든 장치가 온라인으로 연결되어 있다고 가정하지 않는다. 또한 도메인 안에 있는 각각의 디바이스는 디바이스를 식별 할 수 있는 고유한 DID(Device Identity)가 있으며, 디바이스 내부에 제조업자가 발행한 인증서와 개인키가 포함되어 있으며, 물리적인 키 유출을 방지하기 위해 Temper Resistant Memory에 저장된다[3]. 그리고 각각의 장치의 성격에 맞는 DRM 에이전트가 디바이스에 설치되어 있다.

3.2 제안한 DRM 모델

제안하는 DRM 모델은 다음과 같은 요소로 구성되어 있다.

- HADM(Home Authorized Domain Manager) - 홈 네트워크 안에서의 디바이스 전체 도메인을 관리하며, 새로운 디바이스를 도메인에 추가하거나, 혹은 디바이스를 제거한다. 사용자는 홈 디바이스들 중 성능이 가장 좋은 디바이스를 선택한다. Active Device의 기능을 포함한다.
- Active Device - DRM 서버로부터 직접 콘텐츠를

다운로드 받을 수 있으며, 라이선스를 재패키징(re-packaging)할 수 있는 모듈을 가지고 있다. 비교적 높은 처리능력을 가진 PC, PDA와 같은 디바이스가 이에 해당한다.

· Passive Device - DRM 서버로부터 직접 콘텐츠를 다운 받을 수 없으며, 비교적 제한된 처리능력을 가진 디바이스로 MP3player, 자동차 오디오등이 이에 해당한다.

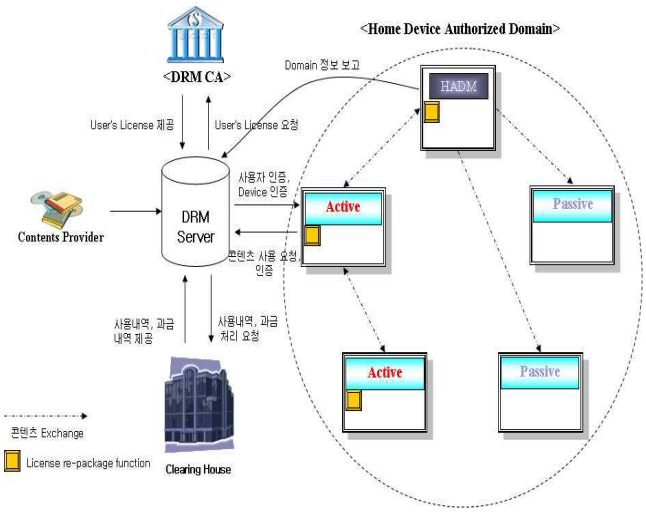

그림 2. 제안한 DRM 시스템 구조

3.3 제안한 시스템의 동작과정

3.3.1 도메인 생성

사용자는 자신이 소유한 디바이스 중 가장 성능이 뛰어한 장치를 선택하여 HADM Agent를 DRM 서버로부터 다운받아 설치한다. HADM 디바이스는 자신의 DID와 Timestamp를 연접하고 해쉬하여 고유한 Domain ID = H(DID||Timestapm) 값을 만든다. 그리고 각각의 장치들이 사용하게 될 Device Key 값을 생성하는데, 집에서 사용하게 될 장치들이 최대 20개 이하일 것으로 가정하고 AES 암호화 방법을 사용하여 128bit 크기의 Device Key를 20개를 생성한다. 그리고 각각의 Key는 LDI(Local Device Index)로 구분이 되며 LDI는 0부터 19까지의 범위를 갖는다. 도메인에 디바이스를 등록할 경우 디바이스는 자신이 사용해야 되는 Key의 LDI를 부여 받는다.

3.3.2 디바이스 등록

최초 사용자가 디바이스를 HADM에 등록하고자 할 때 아래의 그림과 같은 진행과정을 거친다.

· 용어 정리

$Cert_a$: a의 인증서

$nonce_a$: Secret Key를 생성하기 위한 a의 난수

H() : 해쉬 함수

$[message]_{pub\_a}$: message를 a의 공개키로 암호화

$[message]_{sk}$: message를 Secret Key(대칭키)로 암호화

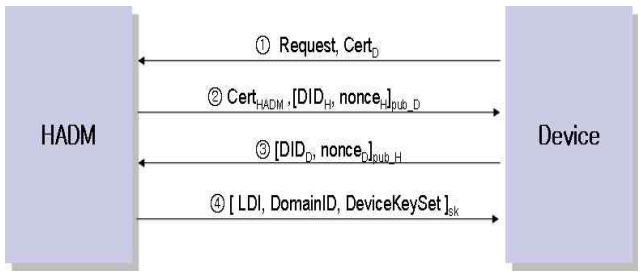

그림 4. 디바이스 등록 프로토콜

① Device는 HADM에게 자신의 인증서와 함께 등록 요청 메시지를 보낸다.

② HADM은 자신의 인증서와 함께 DID, 난수 nonce를 Device의 공개키로 암호화 하여 보낸다.

③ Device는 자신의 DID와 난수 nonceD를 HADM의 공개키로 암호화하여 보낸다. HADM과 Device는 nonceH와 nonceD를 가지고 Secret Key를 생성한다.

④ HADM은 Device에게 Device의 LDI와 전체 DomainID 그리고 Device Key Set를 Secret Key로 암호화 하여 전송한다. 디바이스의 모든 등록 과정을 마치게 되면 HADM은 DRM 서버에게 자신의 Domain 정보를 알린다.

3.3.3 디바이스 상호 인증

콘텐츠를 다운로드 받은 Device는, 같은 도메인 안에 있는 디바이스가 콘텐츠를 요구할 경우, 상호 인증 과정을 거쳐 디바이스에게 콘텐츠와 라이선스 주어야 한다. 아래의 그림은 Device B가 Device A에게 콘텐츠를 요구하는 경우이다.

① Device B는 Device A에게 콘텐츠를 요청 메시지와 자신의 LDI_B 그리고 난수 $nonce_B$를 보낸다.

② Device A는 $nonce_B$와 자신의 Device Key를 연접하고 해쉬하여 SecretKey_A를 생성한다. 그리고 자신의 LDIA, 난수 nonceA와 r, H(r||DomainID)을 SecretKey_A로 암호화 하여 Device B에게 보낸다.

③ Device B는 $[r, H(r||DomainID)]_{SK\_A}$ 를 복호화하

여 Device A가 같은 도메인 안에 있는 디바이스인지 검증을 한다. 만일 같은 도메인 안의 디바이스라면 nonceA와 자신의 Device Key를 연접하고 해쉬하여 SecretKey_B를 생성한 후에 DID_B, r, H(r||DomainID)을 SecretKey_B로 암호화 하여 Device A에게 보낸다.

④ Device A는 $[DID_B, r, H(r||DomainID)]_{SK\_B}$ 를 복호화하여 Device B가 같은 도메인의 안에 있는 디바이스 인지 검증을 한다. 같은 도메인의 디바이스라면, DRM 서버로부터 받은 암호화된 콘텐츠와 Device B의 DID정보에 맞게 재 패키징된 라이선스를 Device B의 Device Key로 암호화하여 Device B에게 보낸다.

3.3.4 라이선스 이동

라이선스가 디바이스 사이를 옮겨갈 때마다, 라이선스는 DID에 맞게 재 패키징 된다. 그러나 Passive 디바이스는 제한된 처리능력으로 인해 재 패키징을 할 수 없으므로 라이선스의 이동은 아래의 표와 같은 제약이 따른다.

표 1. 라이선스 이동 가능여부

라이선스 이동방향	가능 여부
Active → Active	○
Active → Passive	○
Passive → Active	×
Passive → Passive	×

3.3.5 디바이스의 추가, 삭제

디바이스가 추가 되었을 경우 새로운 디바이스는 등록 프로토콜을 통해 도메인에 등록을 한다. 그러나 도메인 안의 디바이스들에게 새로운 디바이스가 추가 되었다는 사실을 알릴 필요가 없다. 왜냐하면 도메인이 생성 시 Device Key를 여러 개 만들었기 때문에 최대 디바이스 개수인 20개를 넘지 않으면 된다.

디바이스가 다른 도메인으로 이동하거나 물리적인 손상, 도난, 해킹을 당했을 경우 도메인 안에서 제거해야 한다. 이때 이 디바이스가 더 이상 도메인에서 사용할 수 없다는 것을 다른 장치들에게도 알릴 필요가 발생하는데, 먼저 HADM이 장치가 제거 되었다는 사실을 DRM 서버에게 알린다. 사용자가 DRM 서버로부터 새로운 콘텐츠를 다운 받을 경우 콘텐츠 안에는 도메인 안에서 사용 가능한 디바이스 DID 목록이 포함되어 있어야 한다. 디바이스에 설치된 DRM Agent는 항상 사용 가능한 Device 목록을 최신의 것으로 유지하여, 콘텐츠의 불법적인 유출을 막아야 한다.

4. 결론

DRM은 콘텐츠의 저작권 보호 기술로써 많은 각광을 받고 있지만, DRM이 가지고 있는 속성들로 인하여 콘텐츠를 사용하는데 있어 많은 제약이 따랐다. 그러나 본 논문에서는 콘텐츠의 공유 가능한 도메인을 정의하고, 디바이스 간에 서로 인증을 하여 콘텐츠를 공유함으로써, 사용자는 콘텐츠의 저작권을 침해하지 않고, 콘텐츠를 보다 자유롭게 사용할 수 있었다. 미래 사회에는 더욱더 다양한 콘텐츠와 이를 사용할 디바이스들이 나올 것이며, 사용자의 편의성은 강조 될 것이다. 향후에는 DRM을 적용하면서도 보다 자유로운 콘텐츠 공유를 위한 다양한 프레임 워크 및 메커니즘 개발에 관한 연구가 필요하다.

참고문헌

[1] DVB - The Digital Video Broadcasting Consortium. http://www.dvb.org

[2] Iwata. T, Abe. T, Ueda. K, Sunaga. H, “A DRM system suitable for P2P content delivery and the studyon its implementation”, Proceeding of the 9th Asia-Pacific Conference on Communications (APCC 2003), Vol. 2, pp. 806-811, 2003 9.

[3] Bogdan C. Popescu, Bruno Crispo, Frank L.A.J. Kamperman, Andrew S. Tanenbaum "A DRM Security Architecture for Home Networks" Proc. 4th ACM Workshop on DRM, pp. 1-10, 2004 10.

[4] S. H. Kwok and S. M. Lui, "A license Management Model to Support B2C and C2C Music Sharing", 10th International World Wide Web Conference, 2001

[5] 박복녕, 김태윤 “디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이센스 관리 프로토콜” 한국정보과학회논문지 VOL.30 NO 02, pp 189~198, 2003. 04